

The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

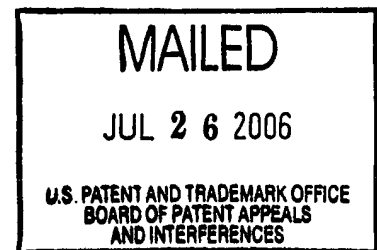
UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte FENG BAO AND DENG HUIJIE

Appeal No. 2006-1566
Application No. 09/623,488

ON BRIEF



Before JERRY SMITH, BARRY, and SAADAT, Administrative Patent Judges.

JERRY SMITH, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on the appeal under 35 U.S.C. § 134 from the examiner's rejection of claims 8-18, which constitute all the claims pending in this application.

The disclosed invention pertains to a method of exchanging digital data between parties over a communications link that uses an off-line trusted party that does not take part in the exchange unless one of the exchanging parties behaves improperly. Specifically, the first party encrypts first digital data and

generates an authentication certificate. The authentication certificate authenticates that the encrypted first digital data is an encryption of the first digital data. The first party then sends the encrypted first digital data and the authentication certificate to the second party.

Using the authentication certificate, the second party verifies that the encrypted first digital data is an encryption of the first digital data. Upon such verification, the second party then sends second digital data to the first party. After verifying the validity of the second digital data, the first party then accepts the second digital data and sends the unencrypted first digital data to the second party.

If the second party verifies that the unencrypted first digital data is valid, it is accepted. If such data is invalid, however, the second party sends the encrypted first digital data and second digital data to a third party that decrypts the first digital data. If the received data is valid, the third party sends the decrypted first digital data to the second party and the second digital data to the first party.

Representative claim 8 is reproduced as follows:

8. A method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data, the method comprising:

the first party encrypting the first digital data and generating an authentication certificate, the authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data, and sending the encrypted first digital data and the authentication certificate to the second party;

the second party verifying that the encrypted first digital data is an encryption of the first digital data using the authentication certificate, and the second party sending the second digital data to the first party when the encrypted first digital data is an encryption of the first digital data;

the first party verifying that the second digital data is valid and, when the second digital data is valid, the first party accepting the second digital data and sending the unencrypted first digital data to the second party;

the second party verifying that the unencrypted first digital data is valid and, when the unencrypted first digital data is valid, the second party accepting the unencrypted first digital data and, when the unencrypted first digital data is invalid, the second party sending the encrypted first digital data and the second digital data to a third party, the third party having a decryption key to decrypt the encrypted first digital data; and

the third party receiving the encrypted first digital data and the second digital data from the second party when the unencrypted first digital data is invalid, the third party decrypting the encrypted first digital data to obtain the decrypted first digital data, verifying that the decrypted first and the second digital data are valid and, when the decrypted first and the second digital data are valid, sending the decrypted first digital data to the second party and the second digital data to the first party.

The examiner relies on the following references:

Angebaud et al. (Angebaud)	5,218,637	Jun. 8, 1993
Micali	5,666,420	Sept. 9, 1997

The following rejection is on appeal before us:

Claims 8-18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Micali in view of Angebaud.

Rather than repeat the arguments of appellants or the examiner, we make reference to the briefs and the answer for the respective details thereof.

OPINION

We have carefully considered the subject matter on appeal, the rejection advanced by the examiner and the evidence of obviousness relied upon by the examiner as support for the rejection. We have, likewise, reviewed and taken into consideration, in reaching our decision, the appellants' arguments set forth in the briefs along with the examiner's rationale in support of the rejection and arguments in rebuttal set forth in the examiner's answer.

It is our view, after consideration of the record before us, that the evidence relied upon and the level of skill in the particular art would not have suggested to one of ordinary skill in the art the obviousness of the invention as set forth in the claims on appeal. Accordingly, we reverse.

Regarding independent claim 8, the examiner's rejection essentially finds that Micali teaches every claimed feature except for the first party sending the unencrypted first digital data after the first party verifies that the second digital data is valid [final rejection, pages 4-6]. The examiner cites Angebaud as teaching a method of exchanging digital data between a first and second party including, among other things: (1) the first party sending encrypted first digital data to the second party; (2) the second party verifying that the encrypted first digital data is an encryption of the first digital data, and the second party sending the second digital data to the first party; (3) the first party verifying that the second digital data is valid and sending the unencrypted first digital data to the second party; and (4) the second party verifying if the first digital data is valid,

and accepting the data [final rejection, page 6]. The examiner finds that it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Angebaud to use secure communication to send unencrypted digital data as taught by Angebaud after verifying the authentication certificate via the exchange of digital signatures as taught by Micali [final rejection, page 6]. According to the examiner, such a modification would minimize the parallel accreditations in each exchange and eliminate the need to authenticate the unencrypted data [final rejection, pages 6 and 7].

Appellants argue that Micali does not disclose nor suggest (1) using an authentication certificate, or (2) that the second party verifies that the encrypted first digital data is an encryption of the first digital using the authentication certificate [brief, page 9]. Appellants note that a digital signature is not the same as an authentication certificate. Also, appellants argue that a digital signature does not necessarily invoke or accompany an authentication certificate [brief, page 12]. To support this distinction, appellants refer to Exhibits "A," "B" and "C" as explaining the differences between an authentication certificate and a digital signature.

According to this evidence, an authentication certificate asserts validity of the binding between the certificate's subject (the key owner) and the subject's public key so that others can be confident that the public key corresponds to the subject who claims the key as their own [brief, page 13]. A digital signature,

however, is a tool for transforming a message via a private key where the data can be verified using the sender's public key [id.].

Turning to the prior art, appellants argue that the mere use of a digital signature by Alice in Micali does not disclose any authentication certificate, let alone the features recited in claim 8 relating to an authentication certificate [id.]. Appellants note that although Alice can digitally sign message "z" (i.e., the encrypted first digital data "m"), Bob does not use Alice's signature to verify that message "z" is an encryption of the first digital data "m". Rather, Alice's signature of "z" merely allows Bob to verify the origin of the message – not to verify that "z" is an encryption of the first digital data "m" [brief, page 14; reply brief, page 7]. Appellants further note that an authentication certificate for private/public keys can be provided at a Certification Authority, and does not require that such an authentication certificate be provided with "z" [brief, page 14].

The examiner broadly interprets the term "authentication certificate" as "[a]n attachment to an electronic message used for security purposes" [answer, page 4]. With this definition, the examiner contends that Micali discloses an authentication certificate to authenticate that an encrypted digital signature is that of a particular party.

Appellants respond that the examiner's definition is overly broad, and the text of claim 8 itself defines an authentication certificate as "'authenticating that the encrypted first digital data is an encryption of the first digital data'" [reply brief,

page 3]. Thus, according to appellants, the “authentication certificate” recited in claim 8 is not a mere verification regarding the sender’s identity (i.e., a digital signature) [reply brief, page 5].

Appellants also argue that, in Micali, after Bob receives the encrypted data “z” from Alice, Bob simply signs “z” and sends it to Alice without authenticating “z” or verifying that “z” is an encryption of “m.” Therefore, the encrypted data string “z” is not itself an authentication certificate and is not accompanied by an authentication certificate [reply brief, pages 8 and 9; brief, page 14].

Appellants further note that no verification exists in Step A2 when Alice sends Bob the encryption of message “m” with Bob’s public key ($E_B(m)$). In that case, Bob merely uses his own private key to decrypt $E_B(m)$ to obtain message “m” [reply brief, page 9]. Thus, there is no reason for Alice to send a separate authentication certificate since Bob already has the message “m” [id.].

We will not sustain the examiner’s rejection of claim 8. We agree with appellants that the combined teachings of Micali and Angebaud do not teach nor suggest an authentication certificate, let alone an authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data as claimed.

In Micali, Alice initially encrypts the message “m” with the Post Office public key of a triplet consisting of identifiers A, B, and the message encrypted in Bob’s key. Such an encryption produces the encrypted data string “z.” Alice then sends “z” to Bob [Micali, col. 5, lines 46-49; Step A1]. When Bob receives

“z,” Bob digitally signs it and sends it to Alice as the receipt [Micali, col. 5, lines 50-51; Step B1]. If Alice receives the properly signed receipt from Bob, she sends Bob the message encrypted in Bob’s key ($E_B(m)$) [Micali, col. 5, lines 52-54; Step A2].

If Alice and Bob are both honest, the process ends at Step A2. Only if Alice fails to execute Step A2 will the trusted third party (i.e., the Post Office) be involved in the transaction [Micali, col. 5, lines 40-45].

We agree with appellants that a digital signature in Micali does not reasonably constitute “authentication certificate” as claimed. As appellants indicate, the language of claim 8 itself requires that the authentication certificate “authenticating that the encrypted first digital data is an encryption of the first digital data.” In Micali, after Bob receives the encrypted data “z” from Alice, Bob simply signs “z” and sends it to Alice without authenticating “z” or verifying that “z” is an encryption of message “m.” At best, Bob’s signature is a mere acknowledgement of receipt of the encrypted data string “z.” Such a mere acknowledgement, however, hardly authenticates that “z” is an encryption of the first digital data “m.” In our view, the encrypted data string “z” is not itself an authentication certificate and is not accompanied by an authentication certificate.

Furthermore, we agree with appellants that an authentication certificate is distinguished from a digital signature essentially for the reasons noted by appellants. But even assuming that an authentication certificate could somehow be construed as a digital signature, we fail to see how Bob (i.e., the second party

in Micali) could possibly verify that the encrypted first digital data is an encryption of the first digital data using the authentication certificate as claimed.

The secondary reference to Angebaud does not cure the deficiencies noted above with respect to Micali. In addition, we see no reason why the first party in Micali (Alice) would send unencrypted first digital data to Bob as suggested by Angebaud since Bob already has the message “m.” That is, after Bob successfully receives $E_B(m)$ from Alice, Bob is able to decrypt the message “m” and the process ends. In our view, there is no reasonable basis to modify Micali using the teachings of Angebaud to send Bob the unencrypted first digital data (“m”) in the manner suggested by the examiner apart from hindsight reconstruction of the claimed invention.

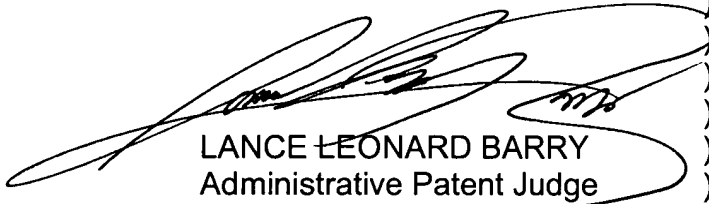
The examiner’s rejection of claim 8 is therefore reversed. Since we do not sustain the examiner’s rejection of independent claim 8, we likewise do not sustain the examiner’s rejection of dependent claims 9-18.

In summary, we have not sustained the examiner's rejection with respect to any of the claims on appeal. Therefore, the decision of the examiner rejecting claims 8-18 is reversed.

REVERSED



JERRY SMITH
Administrative Patent Judge



LANCE LEONARD BARRY
Administrative Patent Judge



MAHSHID D. SAADAT
Administrative Patent Judge

BOARD OF PATENT
APPEALS AND
INTERFERENCES

JS/jaj/kis

Appeal No. 2006-1566
Application No. 09/623,488

GREENBLUM & BERNSTEIN, P.L.C.
1950 ROLAND CLARKE PLACE
RESTON, VA 20191